Palabras del Secretario General de FELABAN Giorgio Trettenero Castro en la apertura del Congreso Latinoamericano de Seguridad Bancaria CELAES

Ciudad de Panamá, Panamá

20 de junio 2019

Sra. Aimee Sentmat Presidente de la Asociación de Bancos de Panama

Sr. Alexis Alcantara Presidente del Comité del CELAES

Sr. Jaime Berry Presidente del Comité Organizador del CELAES

Autoridades, miembros del comité del CELAES, representantes de seguridad de la banca

Buenos días a todos,

Quiero agradecer a todos los asistentes a esta trigésimo cuarta reunión de CELAES. Como todos los años tenemos en nuestro encuentro académico y de negocios concerniente a los temas de seguridad. Agradezco a Panamá, a la asociación bancaria por su invaluable aporte, a todos los integrantes del comité CELAES al comité organizador y a los miembros de la Secretaría General que contribuyeron con este trabajo, para que llegara a feliz término.

La seguridad bancaria es un tema recurrente en todas las épocas. Una de las claves del negocio de la intermediación bancaria tiene ver con la confianza que el público tiene hacia nuestras entidades y nuestra industria.

Diferentes visiones interdisciplinarias (finanzas, economía, psicología) abordan el tema de la confianza con una interrelación entre riesgo y la posibilidad que tiene una empresa de disminuirlo. La banca por definición ha realizado este tipo de acciones toda su vida. Custodia los recursos del público, los protege de la inflación y remunera los mismos a unas tasas de mercado que buscan ser competitivas. Los mantiene en muchos casos disponibles a la vez que realiza la labor de la transformación de plazos para que la identidad básica de la macroeconomía pueda ser una realidad: el ahorro y su conversión en inversión.

La seguridad hoy es determinante en el campo de la informática. Esto porque las transacciones, los servicios, la atención del cliente convergen a este punto. La banca de hoy, exige un nuevo tipo de profesional para convertir sus bancos tradicionales de "sucursales y agencias bancarias" en sistemas simplificados que ofrecen servicios personalizados en

las computadoras portátiles, tabletas y teléfonos inteligentes de sus clientes, y lo que venga en el futuro cercano.

No en vano el economista alemán Klauss Schwab llama esta época la cuarta revolución industrial y al respecto señala: "*estamos al borde de una revolución tecnológica que modificará fundamentalmente la forma en que vivimos, trabajamos y nos relacionamos. En su escala, alcance y complejidad, la transformación será distinta a cualquier cosa que el género humano haya experimentado antes".*

Los cambios requeridos son ingentes. Las inversiones cuantiosas. Desafortunadamente, con la velocidad de los cambios actuales no disponemos de una década para adecuar la industria a los desafíos. El paso debe acelerarse, sino se quiere quedar fuera de los desarrollos más recientes.

A lo largo de la historia hemos protegido los recursos líquidos de la economía de la delincuencia, las hiperinflaciones, las crisis económicas, los proyectos no viables financieramente, entre muchos otros. Hoy la situación no es tan distinta, tan solo que el canal de distribución resulta ser nuevo: **el mundo digital**.

Este avance tecnológico de grandes dimensiones nos lleva a la encarnación de nuevos riesgos que desafortunadamente pueden erosionar el activo mas importante: "la confianza". Una amenaza para el presente y el futuro de nuestra actividad es la aparición y crecimiento del crimen cibernético.

Solo para mencionar algunos:

En noviembre de 2017 el Banco de Inglaterra en su encuesta semestral sobre riesgos, alertó que el sistema financiero local considera los ciber ataques

como el segundo riesgo más grande, solo superado por la crisis del Brexit[1]. Un informe del *Institute of International Finance* (IIF)[2] señaló enfáticamente que los ciber ataques son un problema que puede poner en riesgo la estabilidad financiera. Esto porque hoy existe la posibilidad de ataques a la infraestructura del mercado (sistemas de pagos), robo de datos personales, pérdida de confianza y atentados contra sistemas amplios y transversales como los eléctricos, energéticos o de telecomunicaciones.

La *Office of Financial Research*[3] del Departamento del Tesoro de los Estados Unidos, considera que la ciberseguridad origina problemas relacionados con la continuidad del negocio (riesgo operativo), la destrucción y robo de datos, la pérdida de confianza, los daños físicos en activos de valor financiero y daños

[1] https://www.bankofengland.co.uk/systemic-risk-survey/2017/2017-h2
[2] https://www.iif.com/Publications/ID/228/Cyber-Security-Financial-Stability-How-Cyber-attacks-Could-Materially-Impact-the-Global-Financial-System
[3] https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf

reputacionales a la industria y a las marcas financieras. En esto menciona que en los Estados Unidos la industria financiera es la cuarta más afectada por problemas asociados a esta forma de delincuencia.

El pasado mes de enero pasado el *World Economic Forum* presentó el *Global Risk Report*, en el mismo consideró que para el presente año los ciberataques eran la quinta causa de preocupación del mundo, mientras que los fraudes eran la cuarta causa de inconvenientes para los negocios y las actividades cotidianas[4]. Las preocupaciones crecen y las evidencias de los problemas son innegables.

[4] http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

En los últimos 2 años hemos visto ante la opinión como empresas del tamaño y prestigio de Ticketmaster, Newweg, British Airways, el banco inglés TSB, el banco estadounidense JP Morgan sufrieron perdida de datos. Igualmente, firmas de alcance global como Ebay, Target, Adobe, fueron víctimas de robo de documentos, espionaje industrial, destrucción de programas en prototipo, falsificación de documentos, suplantación de privilegios en los servidores, robo de claves de acceso y transacciones financieras fraudulentas.

Los costos están en proceso de cuantificación que no es definitiva, dado la juventud y novedad del fenómeno, pero existen algunas estimaciones que nos permiten aproximarnos a un orden magnitudes. El reconocido *World Economic Forum*, que estima las pérdidas económicas producidas en América Latina por

los ataques cibernéticos en US$87.940 millones[5], aproximadamente un 1.6% del PIB regional, en 2017, siendo Brasil, México Venezuela y Argentina los países más afectados. Asimismo, el Informe Anual de Ciberseguridad de Cisco 2018 halló que más de la mitad de los ciberataques tienen un costo unitario que sobrepasa los US$500 mil[6]. Según el Instituto Tecnológico de Monterrey los ataques pueden valer 575 mil millones de USD al año 2018. Se espera que para el año 2022 se el mundo requiera al menos 2 millones de personas expertas en el tema[7].

[5] ¿Cómo avanza la ciberseguridad en la banca? Disponible en https://revistaitnow.com/como-avanza-la-ciberseguridad-en-la-banca/

[6] Cisco 2018 – Annual Cybersecurity Report. Disponible en https://www.cisco.com/c/en/us/products/security/security-reports.html#~download-the-report

[7] https://www.jornada.com.mx/2018/11/27/economia/027n2eco#

La firma de seguros inglesa Lloyd´s[8] estimó bajo técnicas de Inteligencia Artificial estimó que la industria financiera podría experimentar pérdidas que oscilan entre los 1200 millones de USD y los 16 mil millones de USD.

La importancia para el sector financiero resulta ser capital. Esto puede ilustrarse en una de las más recientes encuesta de seguridad global de Ernst & Young[9], que incluyó entrevistas a más de 1200 CEO´s y responsables de tecnología de grandes empresas en diversos sectores, reveló que el 89% de los encuestados considera que su estrategia de ciberseguridad no cumple totalmente con las necesidades de su organización. Esta estadística, que

[8] https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2017/cyence/emerging-risk-report-2017---counting-the-cost.pdf

[9] Mayor información en http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2017-18

no es positiva a primera vista, en realidad da cuenta que la gran mayoría de entidades, bancarias inclusive, es consciente que la transformación hacia una banca digital integral no puede darse de forma exitosa sin una estrategia integral de ciberseguridad.

Por todo esto, y con acuerdo unánime de nuestro consejo de gobernadores a nivel latinoamericano, hemos emprendido entre otros, un programa de Formación en Prevención de Riesgos Integrales en Ciberseguridad, el cual apalancara a nivel de conocimiento a nuestros principales directivos dedicados a la seguridad bancaria a poder afrontar de mejor manera este entorno cambiante en los riesgos de la nueva seguridad bancaria, el cual consideramos que todos los países deben hacer parte, entre ellos Panamá por supuesto.

De una manera paralela, quiero comentarles que hemos venido trabajando para apoyar nuestra industria bancaria en la región, en la constitución y formación de un Concentrador de Fraude Regional. Esto como una forma de compartir información, incorporar inteligencia en la detección y prevención oportuna de fraudes y mejores prácticas regionales. Esta iniciativa permitirá tener la tecnología al alcance de todos los bancos e instituciones regulatorias para servir así de centro de acopio a la información relevante para todos los bancos y el sector financiero formal. Es nuestro deseo impulsar herramientas cada vez más precisas y actualizadas a nuestros tiempos que permitan neutralizar esta amenaza propia en el proceso de transformación digital en nuestra región. En una primera etapa para tarjetas de crédito y debito, y en una segunda fase incorporaremos y pondremos a disposición de la banca un CSIRT regional.

En un futuro no muy lejano, es previsible que los gobiernos, los legisladores y los organismos de seguridad por mencionar unos pocos, serán más activos escribiendo normas y requerimientos frente al tema. Razón de más para hoy ser muy activos y estar preparados y anticiparnos de la mejor manera posible. En una reunión con ASBA hace un par de semanas, con respecto al tema de seguridad informática (ciberseguridad) se planteó que en general en la región se ha sido mas reactivo que proactivo. Un propósito de los supervisores en la región es redactar un marco de principios que sirva para planear y evaluar la gestión del supervisor y la banca privada. Nos dicen también que es necesaria además la coordinación entre autoridades y entidades financieras (intercambio de información) sobre los temas que son relevantes en este tema. En este sentido sería mucha utilidad que se reporten los ataques informáticos. Como podrán ver hay que adelantarse a los cambios y es mejor autoregularnos.

Quiero agradecer su atención y damos apertura formal a este congreso CELAES. Esperando que la nuestra propuesta de congreso y los proyectos que comenté sean de su utilidad, tanto a nivel personal y profesional como para las entidades que representamos.

¡Muchas gracias a todosi